Public Key Infrastructure Analysis

Electronic Prescriptions for Controlled Substances

Certificate and CRL Profile

Final Draft 1.0

Prepared for

Drug Enforcement Administration
Office of Diversion Control
600 Army Navy Drive
Arlington, Virginia 22202

March 18, 2002

Prepared by
PEC Solutions Inc.

Table of Contents

Page

Table of Contents

Page

Section 1 — Introduction

This document outlines the minimum information required for the Drug Enforcement Administration's (DEA) Electronic Prescriptions for Controlled Substances (EPCS) Public Key Infrastructure (PKI). It does not address the legal issues associated with the EPCS PKI Architecture.

The profile is based on Internet Engineering Task Force (IETF) Request For Comment (RFC) 2459 X.509 Public Key Infrastructure (PKI) for the Internet," and the Federal PKI (FPKI) X.509 Certificate and CRL Extensions Profile.

1.1 Document Organization

The requirements outlined in Section 2 and 3 represent current standards. These may change over time with the influence of new ideas and technologies. The remainder of this document is organized as follows:

Section 2— Section 2 describes the EPCS PKI requirements, security requirements, and analysis applied to the design of the EPCS digital certificate. Entities being issued certificates covered by this profile include the EPCS Root CA, Subordinate CAs, and Subscribers. This section is a basic reference to the "X.509 Public Key Infrastructure Certificates Profile."

Section 3— Section 3 describes certificate requirements for the DEA EPCS model in specific detail. This section includes information that is vital to the organization of the EPCS digital certificate architecture through defining technical certificate requirements. It also provides a detailed overview of the *EPCS Certificate and CRL Profile Worksheet*, which is included in the *EPCS Certificate and CRL Profile Addendu*m.

Section 4— Section 4 describes the Certificate Revocation List (CRL) requirements for the DEA EPCS model in specific detail. This section includes information necessary to help relying parties determine the validity of a DEA EPCS certificate. It also provides a detailed overview of the *EPCS Certificate and CRL Profile Worksheet*, which is included in the *EPCS Certificate and CRL Profile Addendu*m.

Appendix A— Appendix A defines a reference to Document Acronyms.

Appendix B— Appendix B lists the references used in this document as well as other documents that have led to the decisions made for the DEA EPCS certificates.

Section 2 — Requirements

The certificate profile defined in this document was built using US Federal PKI and industry standards. More generally, this profile describes the certificates to be used in an environment where a subscriber can be identified with a high level of assurance for EPCS transactions.

The mechanisms that decide whether a certificate should or should not be considered a EPCS certificate with regard to legislation and Federal regulation are outside the scope of this document. The most important aspects that affect the scope of this specification are:

- Definition of names and identity information in order to identify the associated subject in a uniform way.
- Definition of EPCS certificate management through the key usage extension.
- Definition of a standardized method to store predefined statements relevant to EPCS certificates.

2.1 Properties

An EPCS certificate defined in this standard is assumed to have the following properties:

- The certificate indicates the *EPCS Certificate Policy* is consistent with liabilities, practices and procedures undertaken by the CA, as discussed in 2.3.
- A certificate is issued to a Root CA, Subordinate CAs, Registrants, and Agents of Institutions.
- The certificate contains an identity based on the legal name of the subject.

2.2 Statement of Purpose

For a certificate to serve as a EPCS certificate, the issuing CA will include information identifying the governing Certificate Policy in the certificates that explicitly defines the intended certificate use. This information will assist subscriber and relying parties in evaluating the risk associated with creating or accepting signatures that are based on a EPCS certificates.

The governing Certificate Policy shall be identified in the certificate using the certificate policies extension. The certificate policies extension shall include a registered OID and a user notice.

2.3 Policy Issues

Certain aspects outlined in the *EPCS Certificate Policy* define the context in which this profile is to be understood and used. It is outside the scope of this profile to specify any

policies or legal aspects that will govern services that issue or utilize certificates according to this profile. The issuing CAs must operate in accordance with the *EPCS Certificate Policy*.

2.4 Uniqueness of Names

The Distinguished Name (DN) must be unique, during the lifetime of the CA, for each Subscriber.

Section 3 — Certificate Profile

EPCS certificates are standard X.509 certificates with special attributes added to support the electronic transmission of controlled substance prescriptions.

3.1 Basic Certificate Fields

Basic certificate fields of the EPCS certificates can be further divided into categories such as issuer DN, subject DN, validity, serial number, etc. Detailed descriptions of formats and accepted attributes can be found in the *EPCS Certificate and CRL Profile Addendu*m. Relying parties MAY have to consult associated certificate policies and/or the issuer's Certificate Practice Statement (CPS), in order to determine the semantics of name fields and the laws under which the issuer operates.

3.1.1 Certificate Information

The certificate must include the certificate X.509 version number, the certificate serial number, and the validity period. The certificate version number for all EPCS certificates will be V3 to represent the X.509 V3 certificate type used. This number can be considered a unique identifier among associated certificates. The validity period consists of two sections that indicate how long a certificate is to be valid. The first section is called “notBefore” and represents the beginning point of the validity period. The second section is called “notAfter” and represents the ending point of the validity period.

3.1.2 Issuer

The issuer field is the identity of the organization responsible for issuing the certificate. The name of the issuing CA must be the officially registered organization name as applied to the DEA.

3.1.2.1 Distinguished Name

The identity of the Root CA is defined as:

C=US, O=U.S. Government, OU=DOJ, OU=DEA, OU=Office of Diversion Control, OU=EPCS, CN=CA

The Subordinate CAs will be responsible for creating both their DN and the DN of the Subscriber as prescribed in the *EPCS Certificate and CRL Profile Addendu*m. However, DEA requires the Subscriber DN to include the Common Name of the individual using the certificate.

3.1.2.2 Signature

The signature of the issuing CA is the algorithm type used to sign the EPCS certificates. The EPCS CAs and Subscribers will require SHA-1 (FIPS 180-1) as the one-way hash function of choice for use with one of the FIPS 186-2 approved signature algorithms. See the *EPCS Certificate and CRL Profile Addendu*m for more detail.

3.1.3 Subject

The subject field is the identity of the Subscriber who is being assigned the certificate from the issuing CA. In the EPCS architecture, the subject can be one of the following participating parties: Root CA, Subordinate CA, or Subscriber. A Subscriber will have first successfully registered with the DEA. Note: The Subscriber may be a Practitioner, Hospital, or others eligible as defined in DEA regulations.

3.1.3.1 Distinguished Name

The identity of the subject must include certain predefined attributes according to organization.

The Root CA must be:

C=US, O=U.S. Government, OU=DOJ, OU=DEA, OU=Office of Diversion Control, OU= EPCS, CN=CA

The subordinate CA shall define their own DN and the subscriber must include the following attribute:

CommonName (Name of Registrant or Agent of Institution as defined by DEA Regulations Sections 1301.22 and 1306.03)

3.1.3.2 Signature Information

The subjectPublicKeyInfo is a basic parameter of the EPCS certificate, used to describe the algorithm and public key of the subject. EPCS Root, Subordinate CAs, and Subscribers will use a FIPS 186-2 approved signature algorithm with SHA-1 hashing. See the *EPCS Certificate and CRL Profile Addendu*m for more detail.

3.2 Standard Certificate Extensions

Certificate extensions are the key attributes that allow EPCS certificates to efficiently integrate new technology with present DEA regulations. The EPCS certificate will include standard X.509 v3 extensions that have been defined in RFC 2459 in addition to additional extensions defined in this document. Making extensions mandatory or critical is addressed differently depending on the extension and how it is used with DEA applications. Participating entities must address the profile worksheet included in the *EPCS Certificate and CRL Profile Addendu*m for more detailed profile requirements.

3.2.1 Authority Key Identifier Extension

The Authority Key Identifier extension identifies the public key used to verify the signature on the certificate. The Authority Key Identifier extension provides a means of identifying the public key corresponding to the private key used to sign a certificate. Since the extension is considered to be an efficiency-enhancing certificate extension within FPKI standards, it is marked as required. This extension must be marked non-critical.

Root CA Certificate	This extension MUST be included
Subordinate CA Certificate	This extension MUST be included
Subscriber Certificate	This extension MUST be included

3.2.2 Subject Key Identifier Extension

The Subject Key Identifier extension identifies the public key being certified. It allows for differentiation of distinct keys used by the same subject. Since the extension is considered to be an efficiency-enhancing certificate, it is required. This extension must be marked non-critical.

Root CA Certificate	This extension MUST be included with SHA-1 as hash identifier
Subordinate CA Certificate	This extension MUST be included with an standardized hash identifier
Subscriber Certificate	This extension MUST be included with an standardized hash identifier

3.2.3 Key Usage Extension

The Key Usage extension serves to limit the technical purposes for which a public key listed in a valid certificate may be used. Subordinate CAs may issue certificates that contain a key usage extension limiting the keys to signing certificates, certificate revocation lists, and other data. This extension must be marked critical.

Root CA Certificate	This extension MUST be included
Subordinate CA Certificate	This extension MUST be included
Subscriber Certificate	This extension MUST be included

3.2.4 Certificate Policies Extension

The Certificate Policies extension lists the supporting CA Certificate Policy OID, as well as optional qualifier information pertaining to these policies. The qualifier is a method of adding text information directly into the certificate. The information could represent a legal statement or CP website information. The extension is processed by relying party applications during the certificate path validation process. This extension must be marked as non-critical.

Root CA Certificate	This extension MUST be included
Subordinate CA Certificate	This extension MUST be included
Subscriber Certificate	This extension MUST be included

Subordinate CA certificates shall include the user notice qualifier containing an explicit text notice.

3.2.5 Subject Alternative Name Extension

The Subject Alt Name extension provides a name that is bound by the Root-CA or CA to the subject's certified public key. This extension must be marked as critical.

Root CA Certificate	This extension MUST NOT be included
Subordinate CA Certificate	This extension MUST NOT be included
Subscriber Certificate	This extension is OPTIONAL

3.2.6 Basic Constraints Extension

The Basic Constraints extension identifies whether or not the certificate belongs to a CA and how many entities the certification path permits through that CA. When pathLenConstraint does not appear, there is no limit to the allowed length of the certification path. This extension must be marked as critical.

Root CA Certificate	This extension MUST be included
Subordinate CA Certificate	This extension MUST be included
Subscriber Certificate	This extension is OPTIONAL

3.2.7 CRL Distribution Points Extension

The CRL Distribution Points extension identifies how the relying party obtains CRL information. EPCS certificates can use LDAP URL, HTTP URL, or DN syntax to access CRL information. This extension must be marked as non-critical.

Root CA Certificate	This extension MUST NOT be included
Subordinate CA Certificate	This extension MUST be included
Subscriber Certificate	This extension MUST be included

3.2.8 Authority Information Access Extension

The Authority Information Access extension indicates how to access issuing CA information and services. Information and services may include on-line validation services and CA policy data. This extension must be marked as non-critical.

Root CA Certificate	The use of this extension is OPTIONAL
Subordinate CA Certificate	The use of this extension is OPTIONAL
Subscriber Certificate	The use of this extension is OPTIONAL

3.2.9 Private Key Usage

The private key usage period extension allows the certificate issuer to specify a different validity period for the private key than the certificate.

Root CA Certificate	The use of this extension is OPTIONAL
Subordinate CA Certificate	The use of this extension is OPTIONAL
Subscriber Certificate	The use of this extension is OPTIONAL

3.3 EPCS Specific Extensions

The following extensions have been added to support DEA business requirements. These extensions must be included in Subscriber certificates and marked non-critical. Values for the EPCS specific extensions should be consistent to the CSA database and the DEA Form 223.

3.3.1 DEA Certificate Version Number Information

The DEA Certificate Version Number Information extension allows relying party applications to identify the DEA profile version being used by the particular certificate. This enables multiple profile versions to be used at the same time without ambiguity. This profile is version 0.1 and has the printable string format *number.number* (example, 0.1).

3.3.2 DEA Registrant Name

The DEA Registrant Name extension is used to identify the DEA Registrant. The name must be consistent with the Controlled Substance Act (CSA) database Registrant Name and has a printable string format as it appears in the CSA database and the DEA Form 223. Example: *last name first name middle initial* (Doe, John A) or *business name* (Acme, Inc.).

3.3.3 DEA Registration Number

The DEA Registration Number extension is used to identify the assigned DEA Registrant number. The number must be consistent with the CSA database Registrant DEA number and has a printable string format (example, AB1234567).

Individuals that are exempt from registration must have a DEA registration number that is consistent with Title 21 Code of Federal Regulations Part 1300-1399.

For agents of an institution the DEA suffix must be consistent and validated with the current list of internal codes that is maintained by the hospital or institution that has permitted the (agent) individual to dispense, administer, or prescribe drugs within the jurisdiction.

Individual	Institution /Service	Suffix/ identification number	DEA Registration # Value
Jane Doe	AB1234567	JD213452345	AB1234567- JD213452345
John Smith	N/A	N/A	AB12345

Figure 1. DEA Number Values

3.3.4 DEA Valid Schedules

The DEA Valid Schedule extension is a way to enter those schedules the certificate user is authorized to prescribe. The format of information entered into this extension consists of both numeric and alphanumeric information delimited by a dollar sign (example, 2$2n$3$3n$4$5). The below table provides a listing of the codes that represent the allowable controlled substance schedules.

Schedule	Code
Schedule II Narcotic	2
Schedule II Non-narcotic	2n
Schedule III Narcotic	3
Schedule III Non-narcotic	3n
Schedule IV Narcotic	4
Schedule V	5

Figure 2. Controlled Substance Schedule Codes

A listing of Schedules of Controlled Substances is provided in Title 21 Code of Federal Regulations Part 1300-1399.

3.3.5 DEA Business Category

The DEA Business Category extension is used to provide members of the EPCS domain the ability to view what business classification the Subscriber belongs to. The category must be consistent with the CSA database Business Activity Code and have printable string format A*lphanumeric$Alphanumeric*. The format of information entered into this extension consists of alphanumeric information delimited by a dollar sign (example, C). The table below provides a listing of the codes that represent the allowable controlled substance schedules.

Business Activity	Code
Hospital/Clinic	B
Practitioner	C
Mid-Level Practitioner	M

Figure 3. DEA Business Activity Codes

3.3.6 Postal Address

The postal address extension identifies the postal address associated with the registrant, as indicated in DEA Form 223 (DEA certificate of registration). The postal address must be consistent with the postal address extension syntax definition defined by RFC 2252. The values entered into the postal address extension must be consistent with the current values held in the CSA database. The value will be a printable string format delimited by a dollar sign for each value held in the respective address fields of the CSA database. The CSA database fields that represent the postal address are:

- Address 1
- Address 2
- Address 3
- City

- State
- Zip Code

The resulting extension value takes the format of: *Address 1$Address 2$Address 3$City$State$Zip Code*. If a CSA database field value is not present it is omitted while leaving the delimiter fields. Example:

CSA Database Field	CSA Database value
Example 1	
Address 1	Dept 1
Address 2	123 Main Street
Address 3	PO Box 45678
City	Home Town
State	MD
Zip Code	12345-6789
Extension Value	Dept 1$123 Main Street$PO Box 45678$Home Town$MD$12345-6789
Example 2	
Address 1	123 Main Street
Address 2	
Address 3	
City	Home Town
State	MD
Zip Code	12345-6789
Extension Value	123 Main Street $$$Home TownMD12345-6789

Figure 4. Postal Address Example Values

Section 4 — CRL Profile

A Certificate Revocation List (CRL) will make available to all relying parties. A CRL is a list of all revoked certificates of both End Entities and Certificate Authorities and is composed of a sequence of required field information that describes the CRL, revoked certificates, and the periods a CRL will be updated.

4.1 tbsCertList

The first field in the sequence is the tbsCertList or "to be signed certificate list." This field is itself a sequence containing the name of the issuer, issue date, issue date of the next list, the list of revoked certificates, and CRL extensions. Furthermore, each entry on the revoked certificate list is defined by a sequence consisting of certificate serial number, revocation date, and optional CRL entry extensions.

4.1.1 Version

The version field describes the version number of the encoded CRL. Since extensions are duplicative as required by this profile, this field MUST be present and MUST specify version 2 (the integer value is 1).

4.1.2 Signature

The signature field contains the algorithm identifier for the algorithm used to sign the CRL. This field MUST contain the same algorithm identifier as the signatureAlgorithm field in the sequence CertificateList (section 4.2).

4.1.3 Issuer Name

The issuer name field identifies the entity that has signed and issued the CRL. The issuer identity is contained in the issuer name field. The issuer name field MUST contain an X.500 distinguished name (DN). The issuer name field is defined as the X.501 type Name, and MUST follow the encoding rules for the issuer name field in the certificate (see Certificate Profile section 3.1.2).

4.1.4 This Update

The "this update" field indicates the issue date of the CRL. Certificate Authorities conforming to this profile MUST encode thisUpdate as UTCTime for dates through the year 2049. Where encoded as UTCTime, thisUpdate MUST be specified and interpreted as defined in Certificate and CRL Profile Worksheet provided in the *EPCS Certificate and CRL Profile Addendu*m.

4.1.5 Next Update

The "next update" field indicates the date by which the next CRL will be issued. The next CRL could be issued before the indicated date, but it will not be issued any later than the

indicated date. This profile requires inclusion of nextUpdate in all CRLs issued by conforming Certificate Authorities. A CAs conforming to this profile MUST encode nextUpdate as UTCTime for dates through the year 2049. Where encoded as UTCTime, nextUpdate MUST be specified and interpreted as defined in Certificate and CRL Profile Worksheet, *EPCS Certificate and CRL Profile Addendu*m.

4.1.6 Revoked Certificates

The revoked certificates field is comprised of a list of all certificates a Certificate Authority has revoked. The certificate serial number and the date on which the revocation occurred uniquely identify revoked certificates. The time for Revocation Date MUST be expressed as described in section 4.1.4.

4.1.7 Extensions

The X.509 v2 CRL format also allows communities to define private extensions to carry information unique to those communities. Each extension in a CRL may be designated as critical or non-critical.

4.1.7.1 Authority Key Identifier

The authority key identifier extension provides a means of identifying the public key corresponding to the private key used to sign a CRL. The identification can be based on the key identifier (the subject key identifier in the CRL signer's certificate) or on the issuer’s name and certificate serial number. This extension is especially useful when an issuer has more than one signing key, either due to multiple concurrent key pairs or due to changeover. Conforming Certificate Authorities MUST use the key identifier method, and SHOULD include this extension in all CRLs issued.

4.1.7.2 CRL Number

The CRL number is a non-critical CRL extension. It is used to convey a monotonically increasing sequence number for each CRL issued by a CA. This extension allows users to easily determine when a particular CRL supersedes another CRL. A CAs conforming to this profile SHOULD include this extension in all CRLs.

4.1.7.3 Delta CRL Indicator

The delta CRL indicator is a critical CRL extension that identifies a delta-CRL. The use of delta-CRLs can significantly improve processing time for applications that store revocation information in a format other than the industry standard CRL structure. This allows changes to be added to the local database while ignoring unchanged information that is already in the local database. This extension is OPTIONAL.

4.1.7.4 Issuing Distribution Point

The issuing distribution point is a critical CRL extension that identifies whether the certificate revocation list is for end-entity certificates, CA certificates, or contains a

limited set of reason codes. CAs conforming to this profile SHOULD include this extension in all CRLs.

4.2 Signature Algorithm

The signature algorithm field contains the algorithm identifier for the algorithm used by the CA to sign the CertificateList. The field is of type AlgorithmIdentifier, which is defined in the Certificate Profile as being a FIPS 186-2 approved algorithm.

4.3 Signature Value

The signature value field contains a digital signature computed upon the ASN.1 DER encoded tbsCertList. The ASN.1 DER encoded tbsCertList is used as the input to the signature function. This signature value is then ASN.1 encoded as a BIT STRING and included in the CRLs signature value field.

Appendix A — Document Acronyms

CA	Certification Authority
CN	Common Name
CONOPS	Concept of Operations
COTS	Commercial Off The Shelf
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSA	Controlled Substances Act
DEA	Drug Enforcement Administration
DN	Distinguished Name
FIPS	Federal Information Processing Standard
FPKI	Federal Public Key Infrastructure
ID	Identification
IETF	Internet Engineering Task Force
IP	Internet Protocol
LDAP	Lightweight Directory Access Protocol
NIST	National Institute of Standards & Technology
PEC	Performance Engineering Corporation
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure for X.509
RA	Registration Authority
RFC	Request For Comment

RSA	Rivest, Shamir, & Adleman
Rx	Prescription
TCP/IP	Transmission Control Protocol / Internet Protocol
UID	Unique Identifier
X.500	The standard for directory services
X.509	The standard for PKI certificates

Appendix B — References

[CONOPS] *Electronic Prescriptions for Controlled Substances Concept of Operations*, Drug Enforcement Administration, September 1, 2000

[EPCSCP] *Electronic Prescriptions for Controlled Substances Certificate Policy PKI Draft Revision 3*, Drug Enforcement Administration, October 31, 2001

[RFC3039] *Internet X.509 Public Key Infrastructure Qualified Certificates Profile*, Internet Draft <draft-ietf-pkix-qc-06.txt>, January 2001

[RFC2459] *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, Network Working Group, January 1999

[DRAFT] *Internet X.509 Public Key Infrastructure Certificate and CRL Profile*, Network Working Group, January 2002

[ITU-T] *X.680: Information Technology - Abstract Syntax Notation One*, X.680 ITU-T Recommendation, 1997.

[RFC822] *Standard for the format of ARPA Internet text messages*, Crocker, D., STD 11, RFC 822, August 1982.

[FPKI] *Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile*, FPKI twg-00-18, April 18, 2000

[XLS] ICSA's PKIX Certificate Profile, Robert Moskowitz, September 6, 1999

[ASTMCP] *Standard Certificate Policy for Healthcare PKI*, ASTM 31.20, April 2, 2001